Scottish Funding Council
Promoting further and higher education

ACC/18/06
Agenda item 9
6 March 2018

Update on preparations for the General Data Protection Regulation

Purpose

1. To invite the Audit and Compliance Committee to review SFC's General Data Protection Regulation (GDPR) Project Plan.

Background

2. The EU General Data Protection Regulation 2016/679 will come into force on 25 May 2018 and represents the biggest change to the data protection landscape in over 20 years. The regulation is an evolution of current data protection law and is underpinned by similar principles, but there are significant changes which will apply to SFC.

3. A high level summary of the changes relevant to SFC brought in by GDPR are:

   - Increased transparency: SFC will need to clearly communicate how we use personal data and for what purposes.
   - More rights for individuals: explicit rights, including the right to deletion of personal data if we are found not to require it and the right to rectification if it is found to be incorrect.
   - Changes to legal bases for processing personal data:
     - Public bodies cannot rely on 'legitimate interests' to process personal data.
     - Requirements for using consent are also much stricter.
   - Requirement to consider 'privacy by design':
     - Requirement to carry out Data Protection Impact Assessments for some projects.
     - Use of personal data must be minimised.
     - Personal data should be anonymised or 'pseudonymised' where possible[1].
   - Definition of personal data is broader: data will now be considered personal if anyone can reasonably use it to identify someone, not just the organisation which holds it.

[1] Pseudonymisation is a new term to the GDPR which describes data which is partially anonymised but could be linked back to personal data using information held elsewhere

- Data Breaches must be reported to the Commissioner's Office if they are considered 'high risk'.
- Higher fines for data breaches: fines will increase from a maximum of £500k under current legislation to a maximum of €20 Million.
- Requirement to appoint a Data Protection Officer (DPO): the role of the DPO is to oversee data protection compliance in the organisation and he or she must be appropriately involved in decisions regarding use of personal data.

The Project Plan

4. SFC processes large volumes of personal data, including data of FE students, HE and FE institutions' staff and SFC staff. SFC also shares data with third parties including other public sector organisations, as well as the private sector.

5. The project plan identifies the main changes that GDPR will introduce and identifies what actions will need to be made in order to achieve compliance with the new regulations in processing this personal data.

6. The plan is a living document and is intended to be amended throughout the life of the project as progress is made and new challenges are identified. The copy provided is up to date as of 20 February 2018

Preparing for GDPR

7. Although the GDPR regulation is finalised and will be implemented on 25 May 2018, the associated UK Data Protection Bill is still going through the House of Commons and is subject to change. Therefore, some aspects of the new regime are still unclear, such as the types of information which might be exempt from GDPR.

8. Additionally, the EU Article 29 Working Party – which provides the European Commission with independent advice on data protection matters – and the UK Information Commissioner's Office (ICO) are still to finalise and publish certain pieces of key guidance and interpretations of GDPR, which may influence best practice.

9. The project is therefore expected to continue beyond 25 May 2018 as further guidance is published and other compliance issues are identified. The Information Commissioner has acknowledged that organisations '…will be expected to continue to identify and address emerging privacy and security risks in the weeks, months and years beyond May 2018.' However she also made it clear that there will be no 'grace period' when it comes to enforcing compliance.[2]

[2] Elizabeth Denholm, Information Commissioner, 'GDPR is not Y2K', ICO blog, https://iconewsblog.org.uk/2017/12/22/gdpr-is-not-y2k/, accessed 20/02/2018

10. Some of the most significant changes which we propose to make are summarised below:

    - Knowing what personal data we hold and for what purposes: we need to establish a central register of the personal data that we process and establish an understanding of the legal bases for processing different categories of personal data.
    - Establishing comprehensive and up-to-date data sharing agreements in place which comply with the new requirements introduced by GDPR.
    - Establishing a central register of data processors used by SFC.
    - Ensuring that we do not keep personal data longer than necessary, particularly by deleting personal data in line with SFC Retention Schedules.
    - Ensuring that staff are aware of, and appropriately trained, in the implications of GDPR.

Risk assessment

11. This paper and the associated GDPR Project Plan are intended to mitigate the risk that SFC is not compliant fully with the requirements of GDPR and, therefore, is not handling personal data in line with the new legal and regulatory regime.

Equality and diversity assessment

12. There are no equality and diversity issues associated with this paper.

Recommendations

13. The Audit and Compliance Committee is invited to provide comment the GDPR project plan and associated risks of non-compliance.

Financial implications

14. There are no direct financial implications arising from this paper however issues identified during the project may have future financial implications.

Publication

15. This paper will be published on the SFC website.

Further information

16. Contact: Callum Morrison, Information Management and Governance Officer (tel: 0131 313 6566; email: cmorrison@sfc.ac.uk.)